



## מתודולוגיית דירוג סיכונים

הודעה בדבר זכויות יוצרים: התוכן זמין בכפוף לרישיון [a Creative Commons 3.0 License](https://creativecommons.org/licenses/by/3.0/)

3.....	מתודולוגיית OWASP לדרוג סיכונים
3.....	כללי
3.....	גישה
3.....	שלב 1 – זיהוי הסיכון
4.....	שלב 2 – גורמים להערכת הסבירות
4.....	קבוצות סיכון
4.....	חולשות
5.....	שלב 3 – גורמים להשפעה
5.....	גורמי השפעה טכניים
6.....	גורמי השפעה עסקיים
7.....	שלב 4 – קביעת חומרת הסיכון
7.....	השיטה הבלתי פורמלית
7.....	השיטה המחזורית
8.....	קביעת החומרה
8.....	שלב 5 – לקבוע מה נדרש לתקן
8.....	שלב 6 – התאמת הסיכון למודל העסקי או האפליקציה
8.....	הוספת גורמים
9.....	התאמת אופציות
9.....	משקל הגורמים
10.....	נספחים

## מתודולוגיית OWASP לדירוג סיכונים

### כללי

✓ מציאת פגיעויות באפליקציות העסק הינה דבר חשוב, אך מדידת הממצאים מול פוטנציאל הנזק העסקי הינה חשובה לא פחות. בימים עברו, בדיקות אבטחה נעשו על ארכיטקטורה או עיצוב על בסיס מודל סיכונים. לאחר מכן, בדיקות אבטחה נעשו על קריאת הקוד או על ידי בדיקות חזרות. פגיעויות אבטחה מתגלות גם כאשר האפליקציה בסביבת העבודה וכבר נפגעה בצורה כזו או אחרת (זמן אמת).

על ידי מעקב אחר הוראות הכתובות במסמך זה, ניתן להעריך את סבירות הסיכונים לתא העסקי ולגבש תכנית עדכנית לטיפול בסיכונים אלו. שיטת הערכת סיכונים חוסכת זמן ותורמת למיקוד ותיעודף לתיקון הסיכונים שנמצאו. תכנית זו תעזור להבטיח שהעסק לא יוסח מטיפול בסיכונים גדולים מסיכונים מינוריים יותר.

### גישה

ישנן גישות שונות לניתוח סיכונים. גישת OWASP המוצגת כאן מבוססת על מתודולוגיות ידועות ובסיסיות אך מכוונות לאבטחת אפליקציות. אז הבא נתחיל במודל הסיכונים הרגיל:

סיכון = סבירות \* השפעה

הגורמים שמרכיבים את הסבירות וההשפעה על אבטחת אפליקציות מפורטים בסעיפים הבאים. על הבודק להבחין ולדעת כיצד לשלבם כדי לקבוע את חומרת וחשיבות הסיכון:

שלב 1: זיהוי הסיכון

שלב 2: גורמים להערכת הסבירות

שלב 3: גורמים להערכת ההשפעה

שלב 4: קביעת חומרת הסיכון

שלב 5: לקבוע מה נדרש לתקן

שלב 6: התאמת הסיכון למודל העסקי או האפליקציה

### שלב 1 – זיהוי הסיכון

השלב הראשון הוא לזהות את הסיכון האבטחתי הנדרש לדירוג. על הבודק לאסוף מידע לגבי קבוצות הסיכון המעורבות, סוג ההתקפה שתמומש, החולשה והשפעת ניצול החולשה על גבי האפליקציה במובן העסקי. יש להניח כי יש מספר קבוצות רב של תוקפים או מספר השפעות של התקפה בודדה על האפליקציה. ללא הגבלת הכלליות, מומלץ לנקוט משנה זהירות ולהציב את מצבי הקיצון בעלי ההשפעה הקריטית ביותר בתודעה האבטחתית.

## שלב 2 – גורמים להערכת הסבירות

כאשר הבודק מצא את פוטנציאל הסיכון וברצונו להעריך את חומרתו, השלב הראשון הוא להעריך את הסבירות של הסיכון להתממש. באופן כללי, זו היא הערכה גסה של הסיכוי של הפגיעות הנתונה להיחשף ולהגיע עד כדי ניצול באפליקציה ע"י תוקף. אין צורך לדיוק יתר בהערכה זו. הערכת הסיכון ע"י שלושת דרגות הסבירות: נמוכה, בינונית וגבוהה הינה מספקת.

יש מספר גורמים המסייעים לקבוע את סבירות הסיכון. סט הגורמים הראשון קשור לקבוצות הסיכון המעורבות. המטרה היא להעריך את הסבירות להצלחת מתקפה של קבוצת סיכון מתוך סך כל התוקפים האפשריים. יש להתחשב בכך שמספר קבוצות סיכון יכולות לנצל את אותה החולשה באפליקציה, לכן נדרש לייחס לכל סיכון את "המצב הגרוע ביותר". לדוגמא, סבירות יותר גבוהה שעובד פנימי יהווה תוקף מאשר אנונימי מבחוץ, אך זה תלוי במספר הגורמים ובמוטיבציה.

יש להדגיש כי לכל גורם יש מספר אופציות ולכל אופציה יש סבירות משלה המזרזת בין 0 ל-9. מספרים עלו נועדו להערכת הסבירות הכללית של הסיכון.

### קבוצות סיכון

סט הגורמים הראשון הינו קבוצות הסיכון המעורבות. המטרה היא להעריך את הסבירות של קבוצת סיכון להצלחה במתקפה (על בסיס "המקרה הגרוע ביותר").

כושר

מהי רמת הטכניקה והכישורים של הקבוצה? כישורי בדיקות חדירות (9), כישורי תכנות ותקשורת (6), משתמש בעל יכולות טכניות מתקדמות (5), משתמש בעל יכולת טכנית רגילה (3), משתמש ללא יכולות (1).

מוטיבציה

מהי רמת המוטיבציה של הקבוצה לניצול החולשה? נמוכה ו/או ללא תגמול (1), אפשרות לתגמול או תגמול סביר (4), תגמול גבוה (9).

הזדמנות

אילו משאבים והזדמנויות דרושים לקבוצת הסיכון כדי למצוא ולנצל את החולשה? גישה מלאה או משאבים יקרים (0), גישה או משאבים מיוחדים (4), גישה או משאבים רגילים (7), ללא גישה או ללא משאבים (9).

גודל

מה הוא גודל הקבוצה? מפתחים (2), מנהלי מערכת (2), משתמשים קשורים (4), שותפים (עסקיים או עמיתים לעבודה) (5), משתמשי האפליקציה (6), אנונימיים (9).

### חולשות

סט הגורמים הבא הינו קשור לחולשות המעורבות בסיכון. המטרה היא להעריך את הסבירות לגלות ולנצל חולשה. בהינתן קבוצת סיכון (כפי הכתוב מעלה).

תגלית החולשה

כמה קל לקבוצת סיכון נתונה לגלות את החולשה? כנראה בלתי אפשרי (1), קשה (3), קל (5), בעזרת כלי אוטומטי (9).

ניצול החולשה

כמה קל לקבוצת סיכון נתונה לנצל את החולשה? כנראה בלתי אפשרי (1), קשה (3), קל (5), בעזרת כלי אוטומטי (9).

מודעות החולשה

כמה חולשה זו מוכרת עבור קבוצת הסיכון הנתונה? לא מוכרת (1), חבויה (4), ברורה (6), ידועה לציבור (9).

איתור החדירה

האם ניצול החולשה יאותר? קיים ניטור אקטיבי של החולשה (1), קיים תוצר על בסיס לוגים המעיד על החדירה (3), על בסיס לוגים בלבד (8), ללא לוגים או תיעוד (9).

### שלב 3 – גורמים להערכת השפעה

כאשר מעריכים את רמת השפעה של תקיפה, חשוב לזכור כי ישנן שני סוגים של השפעות. הסוג הראשון הינו "השפעה טכנית" על האפליקציה, הנתונים בה האפליקציה משתמשת והפונקציונליות והשירותים שהיא מספקת. הסוג השני הינו "השפעה עסקית" על העסק והחברה כהשלכה של הפגיעה באפליקציה.

לרבות, השפעה העסקית יותר קריטית. אולם, לעיתים לבדק לא יהיו מספיק מידע על מנת לקבוע ולהבין את ההשלכות של הצלחת ניצול החולשה. במקרה זה, מומלץ לספק מידע טכני רב ומפורט ככל הניתן על מנת לאפשר לשכבת הניהול העסקית להבין את הסיכונים העסקיים.

יש להדגיש כי לכל גורם יש מספר אופציות ולכל אופציה יש סבירות משלה המזורגת בין 0 ל-9. מספרים עלו נועדו להערכת הסבירות הכללית של הסיכון.

### גורמי השפעה טכניים

ניתן לפרק את גורמי השפעה הטכניים לפי סיווג השפעה האבטחתי הקלאסי: אמינות, סודיות וזמינות. מטרה היא להעריך את סדר הגודל של השפעה על המערכת כאשר הפגיעות מנוצלות.

פגיעה בסודיות

מה היא כמות הנתונים העלולה להיחשף ומה רמת רגישותם אילו ידלפו? חשיפת מינימלית של מידע לא רגיש (2), חשיפת מועטה של מידע רגיש (6), חשיפת מידע רגיש רב (7), חשיפת כל המידע (9).

פגיעה באמינות

כמה נתונים עלולים להיפגע ומה היא רמת חומרת הפגיעה? פגיעה מינימלית בנתונים פגיעה (1), פגיעה מינימלית בנתונים נחוצים (3), פגיעה בנתונים נחוצים (5), פגיעה בנתונים רגישים (7), פגיעה בכל הנתונים (9).

## פגיעה בזמינות

אילו תהליך נפגע, כמה חוסר שירות יכול לפגוע בהליך השירות ומהי חומרתו? הפרעה מינימלית של שירות צד (1), הפרעה מינימלית של שירות עיקרי (5), הפרעה קריטית של שירות עיקרי (7), הפרעה קריטית של כל השירותים (9).

## גורמי השפעה עסקיים

ניתן לפרק את גורמי ההשפעה הטכניים לפי סיווג ההשפעה האבטחתי הקלאסי: אמינות, סודיות וזמינות. מטרה היא להעריך את סדר הגודל של ההשפעה על המערכת כאשר הפגיעות מנוצלות

ההשפעה העסקית נובעת מגורמי ההשפעה הטכניים, אך דורשת הבנה עמוקה על השלכות התקריות השונות בהסתמך על השענות העסק על האפליקציה. באופן כללי, נדרש לתמוך בסיכונים על ידי טיעונים מוצדקים הנובעים בהשפעות עסקיות, ביותר כאשר קהל היעד הינו דרג מנהלים ובכירים. אפיון סיכון כסיכון עסקי הינו הצדקה אולטימטיבית להשקעה וטיפול בסיכון.

בחברות רבות ישנה תבנית או מדריך להגדרת סיכונים עסקיים על מנת למקד את אזור העניין בצורה מותאמת לעסק. סטנדרטים אלו עשויים לעזור למקד את בדיקות האבטחה ולהפיק תוצר אפקטיבי יותר לעסק. אילו לא קיים מסמך או מדריך שכזה, נדרש לבצע שיח עם אנשי העסק המודעים להשלכות ולהשפעות העסקיות של כל תקרית על העסק ולהבין את אזור העניין של העסק.

הגורמים הבאים הינם אזורי עניין הנפוצים ביותר. אזורים אלו הם ייחודיים יותר לעסק מאשר לגורמים: קבוצות סיכון, חולשות והשפעות טכניות.

## נזק כספי

איזה נזק כספי יגרם לעסק עקב ניצול החולשה? פחות מערך הטיפול בסיכון (1), השפעה מועטה על הרווח השנתי (3), השפעה משמעותית על הרווח השנתי (7), פשיטת רגל (9).

## נזק תדמיתי

האם ניצול החולשה יגרום לנזק המוניטין בעסק? נזק מינימלי (1), הפסד גדול של לקוחות (4), אובדן המוניטין (5), נזק המותג (9).

## אי-עמידות

כמה אי-עמידה בהסכמים או בזמינות עלולים לפגוע בתדמית העסק? פגיעה מינורית (2), פגיעה מובהקת (5), פגיעה בפרופיל העסק (7).

## פגיעה בפרטיות

כמה פרטי זהות אישיים חשופים מסוגל העסק לספוג? אחד אקראי (3), מאות של לקוחות/משתמשים (5), אלפי לקוחות/משתמשים (7), כל הלקוחות/המשתמשים (9).

## שלב 4 – קביעת חומרת הסיכון

בשלב זה, תוצאת הערכת הסבירות ותוצאת הערכת ההשפעה מתגבשות יחדיו כדי לחשב את רמת החומרה הכללית של הסיכון. הדבר נעשה ע"י תיוג הסבירות וההשפעה לשלוש רמות שונות – נמוכה, בינונית וגבוהה. סולם הדרגות 0 עד 9 בו השתמשנו עד כה יתפצל לשלושה חלקים:

רמות הסבירות והשפעת הסיכון	
נמוכה	0 עד 3
בינונית	3 עד 6
גבוהה	6 עד 9

## השיטה הבלתי פורמלית

במקרים רבים, אין כל פסול בסיקור הגורמים וגיבוש תשובות פשוטות. הבודק צריך לנתח את הגורמים ולזהות את המפתח להפעלת גורמים אלו שמשפיעים על התוצאות. הבודק עשוי לגלות כי הניתוח הראשוני של גורמים אלו היה שגוי בכך שיבין או יגלה היבטים נוספים שלא התחשב בהם לפני כן או שנראו מינוריים בהערכה הראשונית.

## השיטה המחזורית

אם זה נחוץ להגן על הדירוגים שנעשו בשלבים הקודמים או להפוך אותם למחזוריים (בלתי אפשרי לדרג סיכון אחרת), אז יש צורך לחשב את הדירוגים לכדי מקשה אחת.

תחילה, נדרש לשבץ את הדירוגים שגובשו בטבלאות המובנות. יש לחשב את ממוצע של כל הדירוגים לכדי מקשה אחת שתייצג את סבירות הסיכון. לדוגמא:

קבוצות סיכון				חולשה			
רמת כישורים	מוטיבציה	הזדמנות	גודל	תגלית החולשה	ניצול החולשה	מודעות החולשה	איתור החזירה
5	2	7	1	3	6	9	2
הסבירות הכללית=4.375 (בינונית)							

לאחר מכן, על הבודק לחשב את הערכת ההשפעה הכללית. התהליך דומה גם במקרה זה. במקרים רבים התשובה תהיה ברורה, אך על הבודק לבצע הערכה לפי כל הגורמים או לבצע ממוצע בין כל הדירוגים. (הדירוג הסופי יקבע לפי טבלת המוזכרת מעלה). לדוגמא:

גורמי השפעה טכניים			גורמי השפעה עסקיים			
פגיעה בסודיות	פגיעה באמינות	פגיעה בזמינות	נזק כספי	נזק תדמיתי	אי-עמידות	פגיעה בפרטיות
9	7	5	1	2	1	5
ההשפעה הטכנית הכללית=7 (גבוהה)			ההשפעה העסקית הכללית=2.25 (נמוכה)			

## קביעת החומרה

כאשר גובשו הסבירות הכללית וההשפעות הכלליות, ניתן לשלב אותם בכדי לקבל את דירוג החומרה הסופית עבור הסיכון. חשוב לזכור, אם דירוג ההשפעה העסקית הכללית הוא ברמה גבוהה והדבר ברור עבור הבודק, אז יותר כדי להשתמש בהערכה זו מאשר בדירוג ההשפעה הטכנית הכללית. אך אם אין מספיק מידע בכדי לקבוע זאת, דירוג ההשפעה הטכנית הכללית הוא השני ברשימה.

חומרת הסיכון הכללית				
השפעה	גבוהה	בינונית	גבוהה	קריטית
	בינונית	נמוכה	בינונית	גבוהה
	נמוכה	נמוכה/אזכור	נמוכה	בינונית
		נמוכה	בינונית	גבוהה
סבירות				

בדוגמא מעל, הסבירות היא בינונית וההשפעה הטכנית היא גבוהה, לכן לפי הראיה הטכנית נראה כי חומרת הסיכון היא גבוהה. אולם, ההשפעה העסקית היא נמוכה, אז חומרת הסיכון תתויג כנמוכה. דוגמא זו ממחישה כמה הקישור בין ההשפעה העסקית ובין הפגיעויות, אשר הבודק מעריך, כל כך קריטית בקבלת החלטות כדי לסקר סיכון בשל ומועיל. כשל במנגנון זה עלול להוביל לחוסר אמון בין השכבה העסקית ובין גורמי האבטחה (צוותי האבטחה).

### שלב 5 – לקבוע מה נדרש לתקן

לאחר שכל סיכוי האפליקציה סויגו, אלו ישמשו כרשימת מסודרת (לפי חומרת הסיכונים) המורה "מה נדרש לתקן". באופן גורף, הממצאים המדורגים כקריטיים וברמה גבוהה, הם הראשונים שנדרש לתקן. תיקון סיכונים ברמה בינונית ונמוכה, גם אם אלו קלים וזולים לתיקון, אינם תורמים לפרופיל האבטחתי של העסק כאשר ישנם סיכונים ללא טיפול ברמת סיכון גבוהה.

חשוב לזכור כי לא כל הסיכונים מחייבים טיפול, והפסד פיננסי על טיפול הסיכון הוא אינו ההפסד הפוטנציאלי היחיד, אך מצדיק את הטיפול בסיכון. לדוגמא, אילו 100,000 דולר היא העלות למניעת הונאות על סך של 2,000 דולר לשנה לעסק, ידרשו כ-50 שנים לפחות כדי להחזיר את ההשקעה בטיפול בסיכון. אך חשוב לזכור כתוצאה מהנאות אלו ישנו פוטנציאל נזק לשם החברה ומאידיך יעלה לחברה הרבה יותר כסף ומשאבים לתקן ולטפל בנזקים.

### שלב 6 – התאמת הסיכון למודל העסקי או האפליקציה

מודל דירוג סיכונים אשר מותאמת לעסק היא דבר חשוב עבור השיח והעברת הנתונים בין השכבות העסק ובין השכבה האבטחית. קרוב לוודאי שמודל המותאם אישית לעסק המציג בבהירות את חומרת הסיכונים, יפיק תוצר יעיל וממוקד יותר. חוסר מודל שכזה יכול לגרום לוויכוחים מיותרים וארוכים על דירוג הסיכונים ולבזבז זמן וכסף. יש מספר דרכים להתאים מודל לארגון:

## הוספת גורמים

הבודק יכול לבחור גורמים אחרים אשר מציגים בצורה טובה וממוקדת יותר את אזור עניין ומרכז הכובד של הארגון. לדוגמא, אפליקציה צבאית עשויה להכיל גורמי השפעה המקושרים לחיי אדם או למידע מסווג. הבודק עשוי להוסיף גורמים אחרים כמו גורמי סבירות, כגון חלון הזדמנויות של תוקף או חוסר אלגוריתם ההצפנה.



## התאמת אופציות

יש מקבץ אפשרויות המקושרות לכל גורם, אך המודל יהיה אפקטיבי יותר אילו הבדוק יתאים את האפשרויות לעסק. לדוגמא, להשתמש בשמות של צוותים וחברות אחרות עבור סיווג המידע בצורה מותאמת. על הבדוק לשנות את ניקוד האפשרות לפי הסבירות או ההשפעה על העסק. הדרך הטובה ביותר להתאים ניקוד לאפשרות היא להשוות ניקוד המיוצר על ידי המודל ביחד עם דירוג המיוצר על ידי צוות מומחים של העסק.

## משקל הגורמים

המודל מסתמך על כך שכל הגורמים הם שווים בחשיבותם, ניתן להעריך את משקל הגורמים על מנת להדגיש את הגורמים המשמעותיים יותר עבור העסק. דבר זה יהפוך את המודל למעט יותר מסובך כאשר הבדוק מסתמך על משקל ממוצא וחישוב ממוצא ברוב המודל. אך מלבד זאת המתודולוגיה נשארת על כנה. שינוי המשקלים במודל רצוי ואפשרי רק כאשר העסק מכיר ומאשר כי דירוג הסיכון אכן מדויק.

## נספחים

– OWASP Risk Rating Methodology (מקור)

[https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology/](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology/)

– אתר חברת Triad Security

<http://www.triadsec.com/>

הודעה בדבר זכויות יוצרים: התוכן זמין בכפוף לרישיון [a Creative Commons 3.0 License](https://creativecommons.org/licenses/by/3.0/).  
התוכן תורגם ע"י ירדן ירושלמי וטל ארגוני, חברת Triad Security